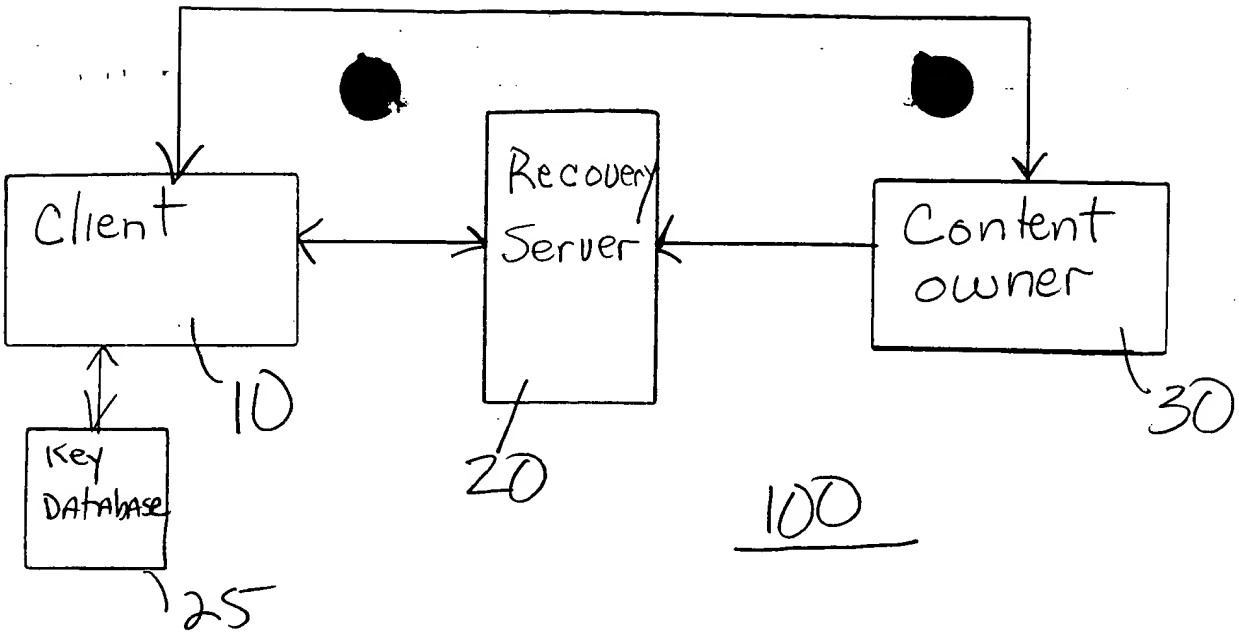
Client
Recovery Server
Content owner
10
20
30
Key Database
25
100

Fig. 1

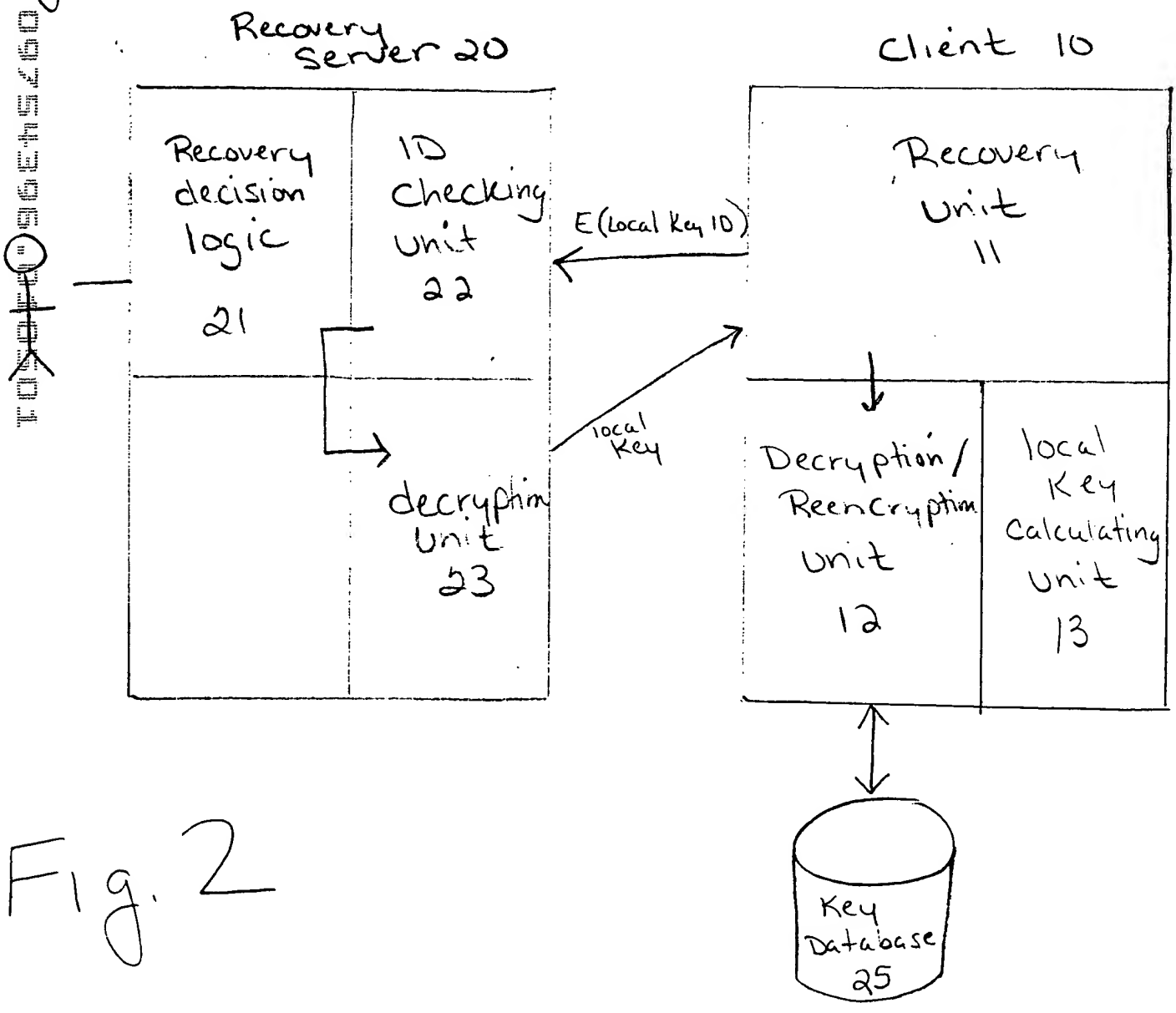
Recovery Server 20
Client 10
Recovery decision logic
21
ID Checking Unit
22
E(local Key ID)
Recovery Unit
11
local Key
decryption Unit
23
Decryption/ Reencryption Unit
12
local Key Calculating Unit
13
Key Database
25

Fig. 2

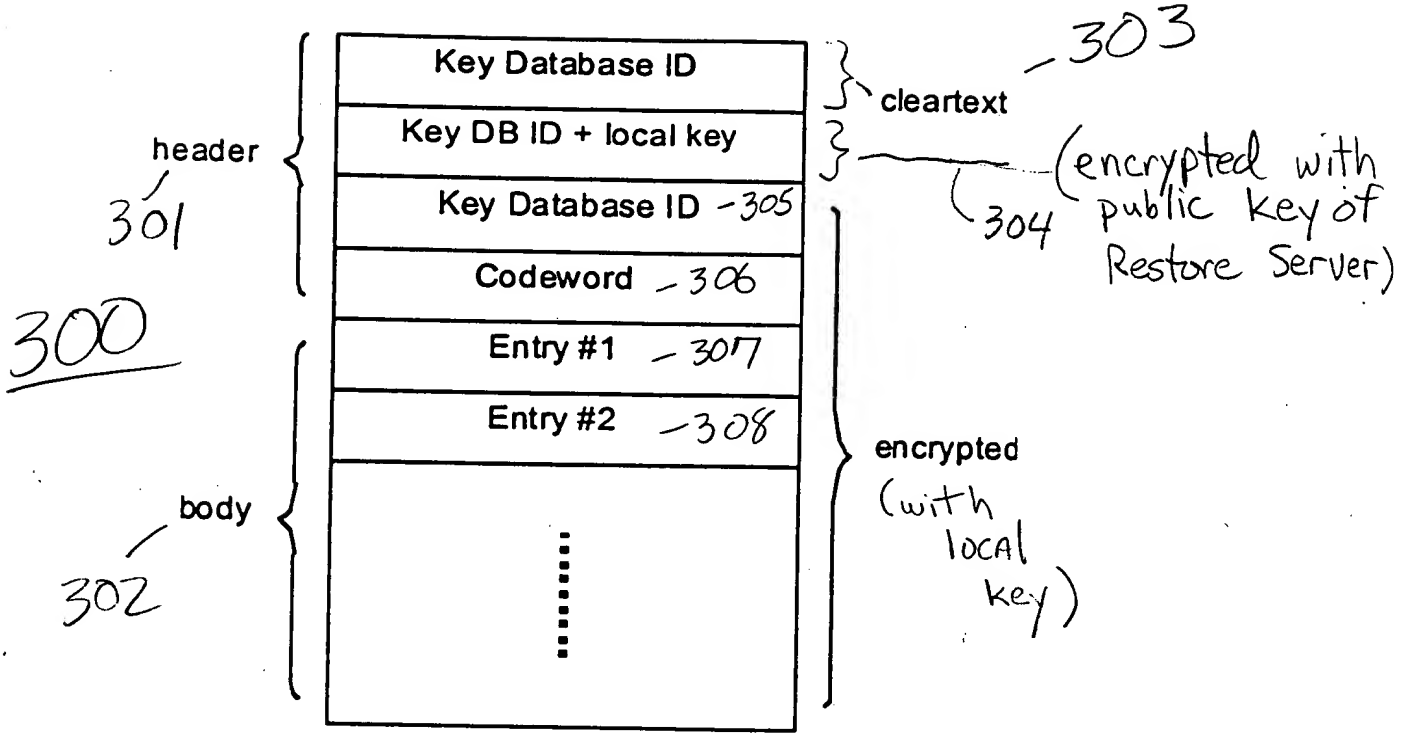
Key Database ID
Key DB ID + local key
Key Database ID -305
Codeword -306
Entry #1 -307
Entry #2 -308
header
301
body
302
300
303
cleartext
(encrypted with public key of Restore Server)
304
encrypted
(with local key)

Fig. 3A

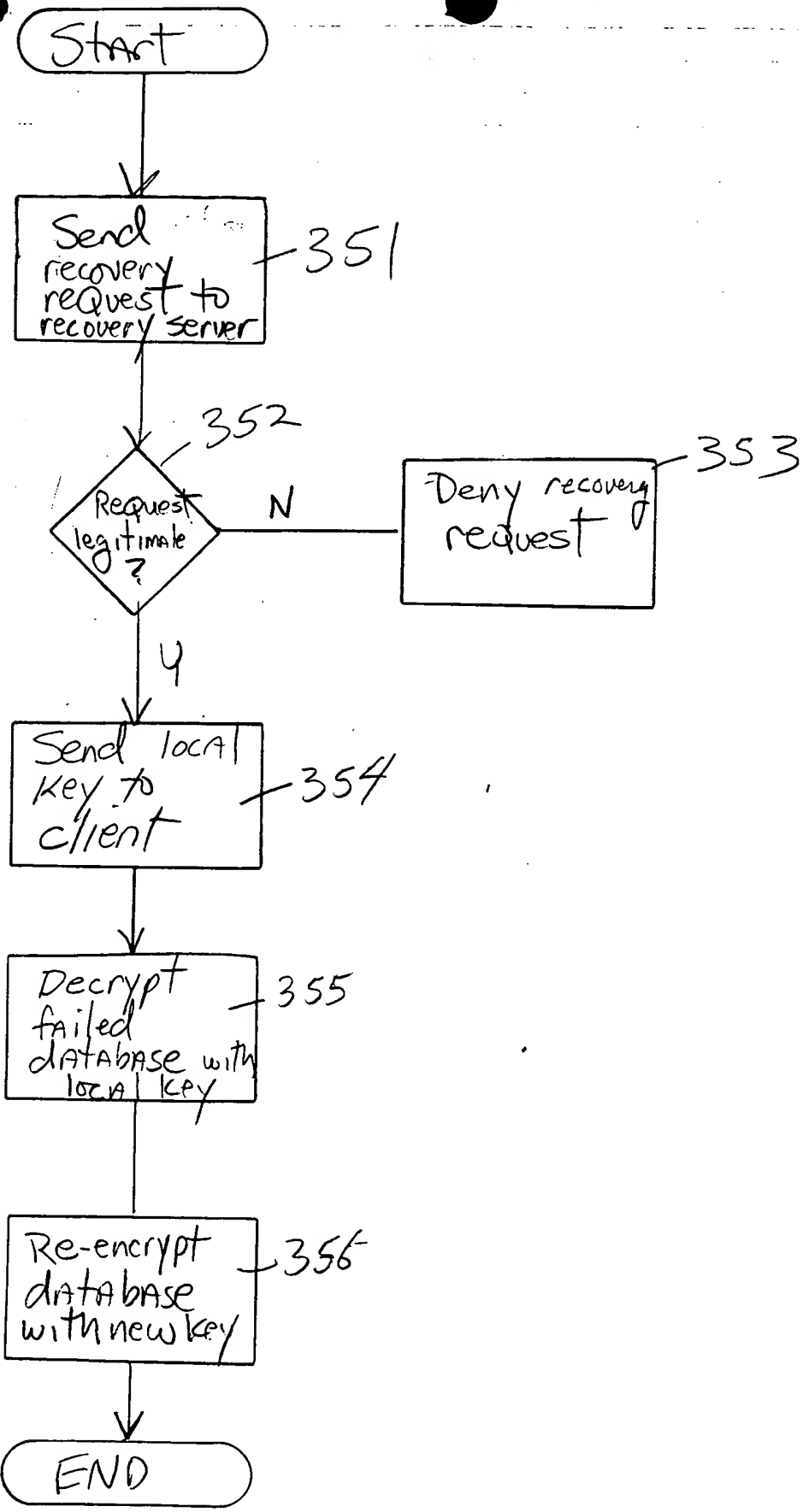
Start
Send recovery request to recovery server
351
350
352
Request legitimate ?
N
Deny recovery request
353
Y
Send local key to client
354
Decrypt failed database with local key
355
Re-encrypt database with new key
356
END

Fig. 3B

TOSOTO" 96EH5260

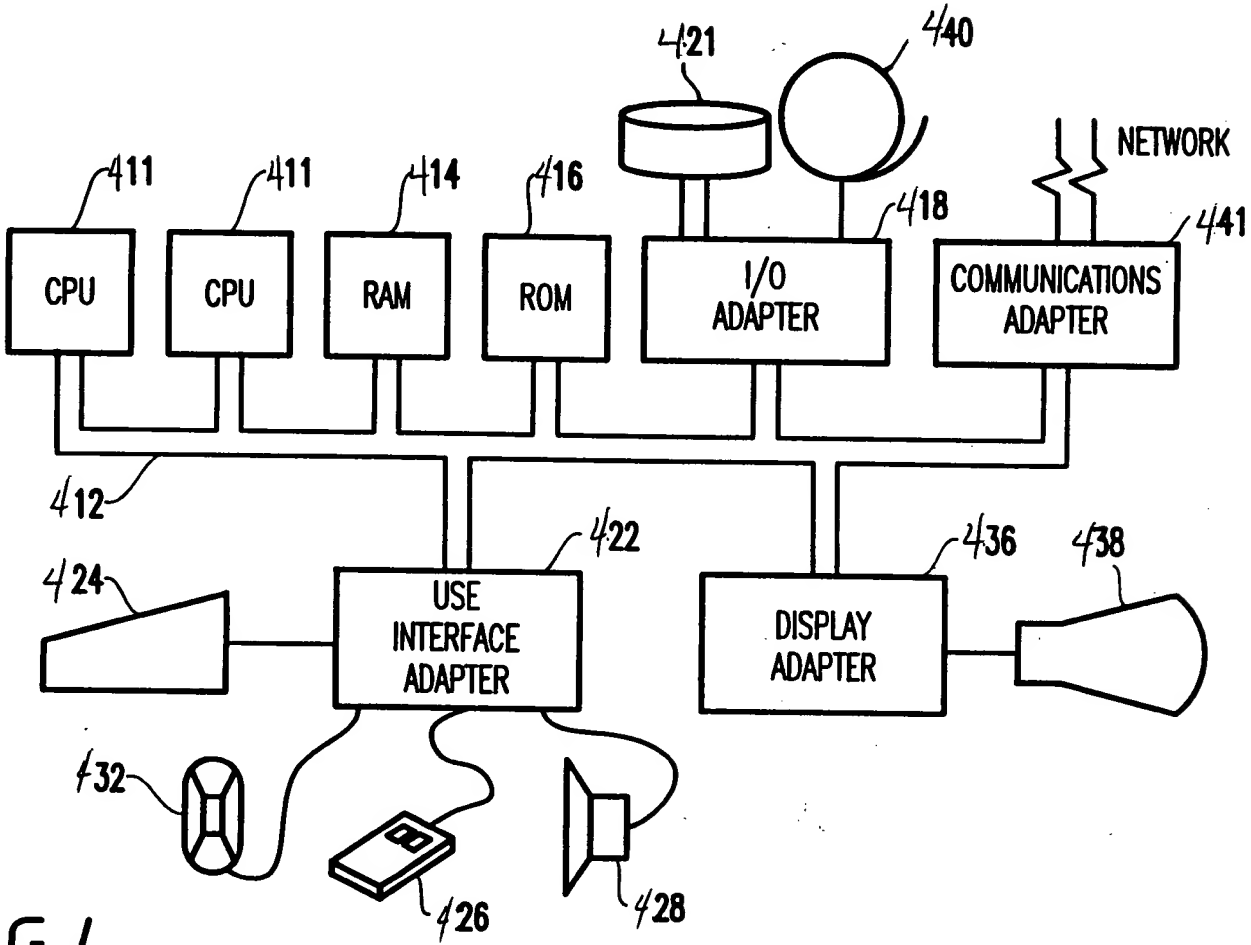

FIG.4

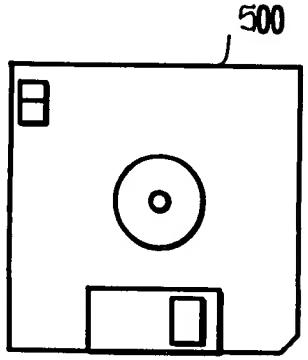

FIG.5